$n, d \in \mathbb{Z}$, $d \neq 0$

$d | n \iff \exists k \in \mathbb{Z}$ s.t. $n = d \cdot k$

$\forall a, b, c \in \mathbb{Z}$, if $a|b$ and $b|c$ then $a|c$

Starting Point: Suppose $a, b, c \in \mathbb{Z}$ s.t. $a|b$ and $b|c$

Show: $a|c$ ($c = a \cdot$ some integer)

Since $a|b$ so $b = a \cdot k$ for some $k \in \mathbb{Z}$

and $b|c$ so $c = b \cdot j$ for some $j \in \mathbb{Z}$

$$
\begin{aligned}
c &= b \cdot j \\
&= (a \cdot k) \cdot j \quad \text{subst.} \\
&= a \cdot (k \cdot j)
\end{aligned}
$$

Let $m = k \cdot j$, $m \in \mathbb{Z}$ since it is the product of ints

so $c = a \cdot m$ where $m \in \mathbb{Z}$

$\therefore$ $a|c$ by def of divides.

QED

Any integer $n>1$ is divisible by a prime number.

$n \in \mathbb{Z},\ n>1$

if n is prime, the statement is true

if n is not prime, then

$n = r_0 \cdot s_0 \qquad r_0, s_0 \in \mathbb{Z}^+$
$1 < r_0 < n$
$1 < s_0 < n$

By def. of divisibility $r_0 | n$

if r_0 is prime, the statement is true

if r_0 is not prime

$r_0 = r_1 s_1 \qquad r_1, s_1 \in \mathbb{Z}$
$1 < r_1 \leq n$
$1 < s_1 < n$

By def of $|$ $\quad r_1 | r_0$

so $r_1 | n$ (since $r_1 | r_0$ and $r_0 | n$)

Keep going until we find r_i that is prime

$1 < r_k < \cdots r_2 < r_1 < r_0 < n$

Unique factorization for integers

Given an integer $n > 1$, there exists a positive integer k and distinct prime numbers $p_1, p_2, \dots p_k$ and positive integers $e_1, e_2, \dots e_k$ such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \dots \cdot p_k^{e_k}$$

and any other expression of n as a product of primes is identical to this except for the order in which they are written.

---

e.g.

$$56 = 2 \cdot 28 = 2 \cdot 7 \cdot 4$$
$$= 2 \cdot 7 \cdot 2 \cdot 2$$
$$= 2^3 \cdot 7^1$$

$$56 = 4 \cdot 14 = 2 \cdot 2 \cdot 2 \cdot 7$$
$$= 2^3 \cdot 7^1$$

Prove or give a counterexample

$\forall a,b \in \mathbb{Z}$ if $a|b$ and $b|a$ then $a=b$

Suppose $a,b \in \mathbb{Z}$ s.t $a|b$ and $b|a$

$b = ka$ for $k, l \in \mathbb{Z}$
$a = lb$

$a = l \cdot b = (l \cdot k) \cdot a$

since $a|b$ and $a \neq 0$

$\cancel{a} = (l \cdot k)\cancel{a}$

$1 = l \cdot k$

$k = l = 1$	$k = l = -1$
$b = k \cdot a = 1 \cdot a = a$	$b = ka = -1 \cdot a = -a$